УДК 343.9

Д. И. Шнейдерова
преподаватель кафедры уголовного процесса
и криминалистики Могилевского института МВД (Беларусь)

АНОНИМНОСТЬ КАК СПОСОБ СОКРЫТИЯ ХИЩЕНИЙ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

Одним из продуктов развития криптовалютной индустрии является новая группа корыстных преступлений, направленных на хищение цифровых валют. Распространение за последние несколько лет получили прежде всего хищение путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации, мошенничество и вымогательство. Согласно статистическим данным информационного центра Министерства внутренних дел Республики Беларусь за 2019 год по стране было зарегистрировано 14 фактов хищений криптовалют, из них 8 приостановлены в связи с отсутствием лица, подлежащего привлечению в качестве обвиняемого, что свидетельствует о наличии некоторых трудностей, с которыми сталкиваются правоохранительные органы при установлении подозреваемого (обвиняемого). Для сравнения в 2018 году был зарегистрирован 1 факт хищения, что также демонстрирует повышенный интерес к криптовалютам со стороны представителей преступного мира.

Привлекательность и популярность криптовалют как мирового средства обмена достигается за счет базовых принципов, заложенных в распределительной системе блокчейн, в которой и происходят их создание и транзакции купли-продажи либо обмена. Первоначально технология блокчейна позиционировалась как децентрализованная, независимая, анонимная и транснациональная система, созданная с целью обеспечить неконтролируемые со стороны государства сделки между ее равноправными участниками, необлагаемые налогами, комиссиями банков и не привязанные ни к территории, ни ко времени. Однако в результате легализации оборота криптовалют некоторыми мировыми государствами последние потеряли свои ключевые свойства. К таким государствам относится и Республика Беларусь, нормативно закрепившая оборот токенов и криптовалюты в конце 2017 года.

С момента легализации любые сделки с криптовалютами на территории Республики Беларусь должны осуществляться физическими или юри-

дическими лицами через криптоплатформы, биржи и обменники, зарегистрированные в качестве резидентов Парка высоких технологий. Кроме того, их деятельность подлежит контролю со стороны Национального банка Республики Беларусь и налогообложению. Таким образом, исключаются принципы децентрализации и анонимности таких сервисов. Если ранее децентрализованность заключалась в отсутствии центрального регулирующего звена всей системы, то есть координирующего и хранящего данные сервера, то теперь, несмотря на т что общий алгоритм работы блокчейна сохраняется (все компьютеры, включенные в систему, хранят базу о совершенных транзакциях), стартовое звено (обладатель криптобиржи) обязано подчиняться нормативным требованиям, а также предоставлять по официальным запросам необходимую правоохранительным органам информацию об участниках и деятельности платформы. Соответственно, ликвидируется и анонимность, так как официальная регистрация, так же как и пользование услугами криптоплатформ, обменников и бирж, требует предоставления от своих участников личных, идентифицирующих их, данных.

Следует отметить, что необходимость нормативного регулирования криптовалюты и придания ей определенного правового статуса была вызвана массовым использованием последней в качестве средства легализации доходов, полученных преступным путем, финансирования террористической деятельности и распространения оружия, наркотических средств, порнографических материалов. В связи с чем контроль со стороны государства за деятельностью криптовалютных сервисов является несомненным преимуществом в работе правоохранительных органов по поиску и установлению лиц, совершивших те или иные преступления, а также обеспечению возмещения причиненного преступлением вреда за счет ареста и последующей реализации криптовалют.

Однако наравне с централизованными криптосервисами продолжают свое существование и осуществляют активную деятельность децентрализованные, созданные за пределами легализовавшего криптовалюту государства. Такие криптоплатформы предоставляют услуги пользователям на основе первоначальных принципов блокчейна, за счет чего пользуются популярностью как у добросовестных пользователей, так и преступников, но создают препятствия для деятельности правоохранительных органов. Рассмотрим механизм их работы.

Для того чтобы стать участником криптоплатформы и совершать в ее пределах транзакции с криптовалютой, необходимо загрузить на свое

устройство (в большинстве случаев это компьютер или съемный винчестер, так как распределительные базы обладают большим весом хранящейся в них информации, но может быть и демоверсия для мобильных устройств) установочный пакет данных. После чего для доступа к базе необходимо придумать логин и уникальный пароль, при этом ввода конфиденциальных данных не требуется, так как их проверка никем не осуществляется. С этого момента пользователь становится участником платформы и может пользоваться ее услугами, в том числе в свободном доступе знакомиться со всеми транзакциями, совершенными внутри сервиса. Каждая транзакция между участниками, чтобы считаться совершенной, должна быть одобрена некоторым количеством иных участников, например десятью. Только после этого запись о ней попадает в блок транзакций. Когда блок накопит необходимое количество записей, он замыкается защитным хэшем, содержащим информацию о предыдущем блоке. Хэш — уникальный ответ, полученный майнером при решении математического алгоритма, за который он к тому же получает награду в виде криптовалют. Связь блоков образует цепочку, изменить данные в блоках которой из-за такого криптографического механизма невозможно, однако ознакомиться с их содержанием может любой участник. Обновление базы транзакций на каждом присоединенном устройстве осуществляется при подключении к сети Интернет. Такой механизм работы обеспечивает децентрализацию, так как отсутствует управляющее звено и все члены равноправны, однако с анонимностью возникают некоторые вопросы в ее объективном понимании.

Рассматривать анонимность только с точки зрения отсутствия личных данных пользователя криптоплатформы (фамилия, инициалы, паспортные данные и т. д.) недостаточно, так как, совершая операции в рамках системы или посредством криптокошельков, пользователь оставляет несколько видов цифровых следов, позволяющих его деанонимизировать. Первая группа следов — данные, хранящиеся в блокчейне о совершенных конкретным пользователем транзакциях, позволяющие связать их между собой и определить источник их реализации (то есть пользователя). Каждая транзакция имеет вход и выход, а также примерное время ее включения в блок (отражается в заголовке блока). Вход позволяет установить источник передаваемых криптомонет, а выход — адрес криптокошелька их получателя и отправляемую сумму. В данном случае следует обратить внимание именно на источник средств, так как в нем заложена ключевая идентифицирующая информация, ведущая к первоначальной точке движения определенной криптомонеты.

Источник средств — это информация о выходе конкретной предыдущей транзакции, то есть источник содержит данные не об адресе кошелька, а о ранее совершенной с криптомонетами сделке. Например, Петров (выход 0) передает Иванову (выход 1) один биткоин. После чего Иванов (вход 1 — информация о транзакции между Ивановым и Петровым, не раскрывающая адреса Петрова) передает этот биткойн Сидорову (выход 2). Сидоров (вход 2 — информация о сделке между Сидоров и Ивановым, не показывающая адрес кошелька Иванова) решает передать этот же биткоин Звонареву (выход 3) и так далее. Таким образом формируется цепочка (граф транзакций), связывающая все транзакции с одной криптовалютой между собой, позволяющая установить первоначального отправителя и движение самой валюты. Идентификация транзакций из общего бесконечного числа достигается за счет присваивания каждой уникального ID-кода при отправке.

Но знания адреса отправителя недостаточно для установления его личности, поэтому на втором этапе необходимо исследовать следы, не записываемые в блокчейне, а именно IP-адрес устройства, которое использовалось сторонами для совершения сделки. Доступность IP-адреса обеспечивается использованием блокчейн платформой незашифрованных пакетов данных, передаваемых по глобальной сети, что позволяет установить его двумя путями: либо через анализ трафика, либо через данные серверов, обеспечивающих работу криптокошельков (аппаратных, программных, онлайн), криптобирж и обменников. По IP-адресу можно установить приблизительное местонахождение пользователя, если проанализировать его через базы данных геолокации IP-адресов, а также интернет-провайдера, предоставляющего услуги по доступу в Интернет, которому известны и личные данные его клиентов. Не стоит исключать и случаи, при которых преступник пользуется не своей (например, домашней) сетью, а общедоступной Wi-Fi, и полагает, что останется необнаруженным. Но в данном случае помощь правоохранительным органам оказывают устройства таких пользователей, хранящие файлы cookie. Последние позволяют связать вход в глобальную сеть с предыдущей историей работы в браузере через ранее использованную сеть и соответственно привязать устройство к конкретному ранее известному IP-адресу. Таким образом, можно прийти к выводу, что описанные цифровые следы за счет общедоступности информации о транзакциях исключают полную анонимность клиента криптоплатформы или иных криптосервисов, что, несомненно, является положительным фак-

тором в процессе розыска преступника, совершившего хищение и обналичивание криптовалюты.

Однако, как и любой высокотехнологичный продукт, криптоплатформы сумели приспособиться под данное обстоятельство и модернизировать свою деятельность в направлении полного обеспечения анонимности клиентов. Так появились анонимные криптоплатформы, не отличающиеся по механизму работы от обычных, за исключением внедрения специального протокола, анонимизирующего данные о совершенных транзакциях. Все анонимные криптоплатформы можно разделить на открытые и закрытые, которые отличаются между собой лишь возможностью доступа к пользованию их услугами (закрытые создаются для нужд ограниченного круга лиц).

Протоколы, обеспечивающие анонимность, также можно классифицировать на четыре вида в зависимости от алгоритма работы: использующие кольцевые подписи, сжигающие монеты, перемешивающие монеты и шифрующие путем доказательства с нулевым значением [1]. В основе использования механизма кольцевых подписей лежит групповое подтверждение совершаемой транзакции, при котором сразу несколько участников платформы подписывают сделку, что не оставляет возможности определить, кто же из них подлинный адресат. Сжигание монет — технология, позволяющая уничтожить связь между данными о входе и выходе криптомонеты за счет ее уничтожения и замены новой, не бывшей в обороте монетой. Криптовалютный миксер, существуя как протокол в рамках платформы, так и в качестве самостоятельного сервиса-анонимайзера сделок, позволяет смешивать поступающие криптомонеты между собой за счет их дробления (процесс запускается при наличии достаточного количества монет), многократного перемешивания и направления конечному адресату. При таком процессе проследить деловые взаимоотношения между отправителем и получателем невозможно. Еще одним средством криптографии, трансформирующим публичные сделки между участниками платформ в анонимные, является протокол-доказательство с нулевым значением. Он позволяет утверждать достоверность транзакции без ее одобрения второй стороной и, соответственно, не раскрывает информацию, за исключением времени совершения сделки. Такая достоверность обеспечивается за счет генерации случайных чисел.

Однако желание большинства пользователей уничтожить следы осуществления каких-либо сделок с криптовалютами в цифровом пространстве привело не только к созданию анонимных криптоплатформ, но и к ис-

пользованию в криптоиндустрии сервисов Tor, позволяющих скрыть IP-адрес пользователя за счет анонимизации трафика. Механизм работы Tor заключается в «луковой» маршрутизации — оперировании случайно выбранными узлами распределенной сети серверов, где каждый из них, получая зашифрованный пакет данных, расшифровывает свой уровень и направляет информацию следующему, и так вплоть до конечного адресата, получающего незашифрованные данные. Следует отметить, что Tor может быть использован как самостоятельный браузер при работе с криптосервисами, так и в качестве дополнительной опции, внедренной в криптоплатформы.

Таким образом, анонимные криптоплатформы и скрытые сервисы предоставляют преимущества хакерам, виртуальным мошенникам и вымогателям, совершающим хищения криптовалют, обеспечивая сокрытие не только их действий, но и данных о личности и местонахождении. Данное обстоятельство препятствует, а в некоторых случаях и вовсе исключает возможность расследования и раскрытия органами дознания и следствия уголовных дел о хищениях в сфере оборота криптовалют. В связи с чем представляется целесообразной разработка правоохранительными органами совместно с интернет-провайдерами, осуществляющими свою деятельность на территории Республики Беларусь, комплекса упреждающих такие факты мер, направленных на ограничение доступа пользователей к нелегализованным криптосервисам (криптоплатформам, биржам и обменникам).

1. Анонимные криптовалюты 2020 [Электронный ресурс] / Информационный портал «ProstoCoin». URL: https://prostocoin.com/blog/anonymity-coins (дата обращения: 31.03.2020). Вернуться к статье